

NIT-200
NT0053US

LIST OF INVENTORS' NAMES AND ADDRESSES

Takeki YAZAKI, Hachioji, JAPAN;

Takeshi AIMOTO, Tokyo, JAPAN.

09585339-050200

NIT-200
NT0053US

United States Patent Application

Title of the Invention

BANDWIDTH MONITORING METHOD AND ITS DEVICE

Inventors

Takeki YAZAKI,

Takeshi AIMOTO.

09585389 060200

BANDWIDTH MONITORING METHOD AND ITS DEVICE

BACKGROUND OF THE INVENTION

Field of the Invention:

5 The present invention relates to a bandwidth
monitoring method for monitoring a bandwidth for each packet
which flows into a network, and a bandwidth monitoring device
therefor.

Description of the Related Art:

10 Traffics (packets), which flow over an Internet, are
increasing rapidly with an increase in Internet users. In
a packet type communication system employed in the Internet,
packets sent from a large number of users can be transmitted
through the use of the same line. It is therefore possible
15 to reduce the cost per bandwidth. With a view toward
achieving the low cost of the packet type communication
system, moves have been made to integrate telecommunication
networks and enterprise networks which have heretofore been
achieved by private networks, into one by the Internet
20 thereby to implement a reduction in communication cost. It
is necessary to implement quality of service (QoS) such as
low latency, low discard probability, etc. which have been
achieved by the conventional telecommunication networks or
enterprise networks for the purpose of integrating these

into one.

As a prior art related to QoS, there is known, for example, a Diffserv (Differentiated Service) (hereinafter called prior art 1) described in RFC2475 of IETF (Internet Engineering Task Force). The prior art 1 describes that traffics (packets) are divided into classes by a source/destination IP address, a source/destination port number, a protocol, etc. in a TCP/IP header at an entrance of a network which provides services, and forwarding operations are assigned thereto. Further, the prior art 1 also describes that each packet is transferred based on a transfer or forwarding operation related to a DSCP (Differentiated Service Code Point) in a header in the network.

A node at the entrance of the network assigns preferentially packet-transferred forwarding operations to packets each of which needs low latency and low discard probability, and each node lying within the network forwards the packets preferentially, whereby the low latency and low discard probability of the packets can be achieved. Incidentally, packets to which preferentially packet-transferred forwarding operations are assigned, and packets other than the packets will be called priority packets and non priority packets respectively.

A network for implementing QoS makes a contract for a bandwidth of priority packets with a user. The node at the entrance of the network has the function of performing bandwidth monitoring and performs monitoring at the bandwidth (bandwidth monitoring or check). The bandwidth monitoring function has been described in, for example, the prior art 1.

The prior art 1 describes that a contract for forwarding-operation decision rules (for example, voice packets are transferred preferentially, etc.), a bandwidth, etc. (TCA: Traffic Conditioning Agreement) is established between the user and the network, and the node at the entrance of the network discards packets or changes DSCP so as to satisfy the TCA. Owing to the bearing of the bandwidth monitoring function by the node at the entrance of the network, a large amount of priority packets sent by one user can be prevented from flowing into the network, and QoS of priority packets sent from other users is achieved.

The bandwidth monitoring function is common as an ATM (Asynchronous Transfer Mode). Bandwidth monitoring executed in the ATM has been described in, for example, Chapter 4.5 of The ATM Forum Specification version 4.0 (hereinafter called prior art 2). In a VBR (Variable Bit Rate) service described in the prior art 2, a user makes

055339 060200

5

10

15

20

20

packets, and voice packets at the monitoring bandwidth or higher and packets other than the voice packets as non priority packets. When traffics sent out by a user are shown in Fig. 8(a), traffics subsequent to the passage of the bandwidth monitoring function are represented as shown in Fig. 8(b). Packets other than the voice packets indicated by diagonally-shaded portions shown in Fig. 8(b) are transmitted as non priority packets regardless of the fact that the priority packets fall within the monitoring bandwidth. Namely, the user is not able to sufficiently use the contract bandwidth for each priority packet.

On the other hand, even the prior art 2 will cause a problem similar to the above. The bandwidth monitoring device having the bandwidth monitoring function according to the prior art 2 transmits only cells with CLP = 0 within the monitoring bandwidth as CLP = 0. When traffics sent out by a user are given as shown in Fig. 15(a), traffics subsequent to the passage of the bandwidth monitoring function are represented as shown in Fig. 15(b). Cells corresponding to the diagonally-shaded portions in Fig. 15(b) are transmitted as cells with CLP = 1 regardless of the fact that the amount of cells with CLP = 0 is within the limit of the monitoring bandwidth. Namely, the user is not able to sufficiently utilize a contract bandwidth with

CLP = 0.

SUMMARY OF THE INVENTION

As described above, the prior art could not provide
 5 such a service that the network operator could effectively
 use the contract bandwidth. Therefore, a first object of
 the present invention is to provide a service allowable ^{by} an
 effective use of a contract bandwidth.

Further, the prior art could not provide a bandwidth
 10 monitoring device capable of providing a service allowable ^{by}
an effective use of a contract bandwidth. A second object
 of the present invention is to provide a bandwidth monitoring
 device by which a network operator is able to provide a
service allowable effective use of a contract bandwidth. ??

15 The first object is solved by the following method.

In a network wherein priority packets each having a
 packet header in which a priority field is set as priority,
 is preferentially transferred as compared with packets other
 than the priority packet, monitoring is carried out on a
 20 bandwidth for each packet flowing into the network for which
 a network operator who manages the network makes a contract
 for a bandwidth of priority packets with a network user
 utilizing the network. When the network user transmits
 priority packets and the other packets to the network, the

09585389.060200

priority fields of some packets other than the priority packets are re-set to a value corresponding to that of the priority field of the priority packet. Described more specifically, when the amount of the priority packets falls
5 within the limit of the contract bandwidth, the priority field of some packets other than the priority packet is rewritten to the value corresponding to that of the priority field of the priority packet.

When the network user transmits packets to the network
10 without setting a value in the priority field and priority packets are determined according to a priority packet decision policy contracted between the network operator and the network user, a value corresponding to the priority field of the priority packet is set to the priority field of some
15 packets judged as non-priority packets.

When the network user transmits packets to the network without setting a value in the priority field and a bandwidth of packets judged as priority packets in accordance with the priority packet decision policy contracted between the
20 network operator and the network user is less than the contract bandwidth, a value corresponding to the priority field of the priority packet is set to the priority field of some packets judged as non-priority packets.

Further, a leaky bucket algorithm having a plurality

002099 695339 060200

of bucket depths is used as an algorithm for the bandwidth monitoring system, and the depth of the bucket is switched in accordance with each input packet.

sub
A1

In order to achieve the second object, a bandwidth
5 monitoring device according to the present invention
comprises flow detecting means for detecting a flow of a
series of packets based on at least one of its address
information, use identification information and network
priority information identifying the priority of the packet
10 in the network, and for determining a flow identifier
indicative of an identifier of each flow and a packet
priority within the flow, a bandwidth check or monitoring
table having one or a plurality of entries each comprising
bandwidth check control information indicative of control
15 information for bandwidth check and a plurality of the
network priorities, bandwidth check table control means for
reading out an entry corresponding to the flow identifier
from the bandwidth check table, check result decision means
for judging whether the input packets conform to or violate
20 the contract bandwidth based on the packet priority,
bandwidth check control information within the entry read
out by the bandwidth check table control means, and a value
of a timer for indicating the present time, and priority
decision means for determining a network priority of the

002090 602000 055389 050200

A1

Further, a bandwidth monitoring device according to the present invention comprises connection priority decision means for determining a packet priority indicative of priority of a packet within the connection from connection information of each input packet, a bandwidth check table having one or a plurality of entries each comprising bandwidth check control information indicative of control information for bandwidth monitoring and network priorities information for identifying a plurality of priorities in the network, bandwidth check table control means for reading out an entry corresponding to an identifier for the connection from the bandwidth check table, check result decision means for judging whether the input packet conform to or violate the contract bandwidth, based on the priority within the connection, bandwidth check control information within the entry read out by the bandwidth check table control means, and a value of a timer for indicating the present time, and priority decision means for determining the network priority of the input packet based on the judging result of the check result decision means and a plurality of network priorities read out by the bandwidth check table

control means.

Furthermore, a bandwidth monitoring device according to the present invention is characterized in that a leaky bucket algorithm having a plurality of bucket depths is used
5 as an algorithm for the bandwidth monitoring to be carried out by the check result decision means, and a bucket depth for priority packets and a bucket depth for packets other than the priority packets are prepared as the bandwidth check control information.

10 Besides, the problems to be solved by the present application and means for solving them will become apparent from the description of the embodiments of the invention and the accompanying drawings.

15 BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing a configuration of a router according to the present invention;

Fig. 2 is a constitutional diagram of an Internet;

Fig. 3 is a diagram depicting a format of a packet
20 employed in the network;

Fig. 4 is a diagram showing a format of a packet processed in the router according to the present invention;

Fig. 5 is a block diagram illustrating a configuration of a bandwidth check unit 141 according to the present

09585389 060200

invention;

Fig. 6 is a diagram depicting a format of a bandwidth check table 550;

Fig. 7 is a flowchart of the bandwidth check unit 141
5 to which the present invention is applied;

Fig. 8(a) is a diagram showing the variation with the passage of time in traffics of voice packets and the other packets transmitted from an enterprise network A210;

Fig. 8(b) is a diagram showing the variation with the
10 passage of time in traffics after passing through a bandwidth monitoring unit to which the prior art 1 is applied;

Fig. 8(c) is a diagram showing the variation with the passage of time in traffics after passing through a router having the bandwidth monitoring unit 141 to which the present
15 invention is applied;

Fig. 9 is a block diagram showing a configuration of a bandwidth check unit 941 to which the present invention is applied;

Fig. 10 is a diagram illustrating a format of a
20 bandwidth check table 950;

Fig. 11 is a flowchart of a check result decision unit 920 to which the present invention is applied;

Fig. 12 is a diagram showing the variation with the passage of time in traffics after passing through the router

09585389.060200

having the bandwidth monitoring unit 141 to which the present invention is applied in a case where four types of traffics are sent out from the enterprise network A210;

Fig. 13(a) is a diagram showing the variation with the
5 passage of time in traffics of priority packets and non priority packets transmitted from the enterprise network A210;

Fig. 13(b) is a diagram showing the variation with the
10 passage of time in traffics after passing through a bandwidth monitoring unit to which the prior art 2 is applied;

Fig. 13(c) is a diagram showing the variation with the
passage of time in traffics after passing through a router having the bandwidth monitoring unit 941 to which the present invention is applied;

15 Fig. 14 is a block diagram illustrating a configuration of a bandwidth check unit 1441 to which the present invention is applied;

Fig. 15(a) is a diagram showing the variation with the
20 passage of time in traffics of CLP = 0 and CLP = 1 transmitted from the enterprise network A210;

Fig. 15(b) is a diagram showing the variation with the
passage of time in traffics after passing through a bandwidth monitoring unit to which the prior art 2 is applied; and

Fig. 15(c) is a diagram showing the variation with the

002090-695555

passage of time in traffics after passing through a bandwidth monitoring unit to which the present invention is applied.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

5 A summary of a router according to the present invention, which has a bandwidth monitoring function, will first be described using Figs. 1, 3 and 4.

Fig. 1 shows a router 100 according to the present invention. The router 100 comprises an input line 101 to
10 which packets are inputted, a packet receiving circuit 160 for performing processing to receive the packets, M buffers on receiving side 130-i (where $i = 1$ to M), a buffer selector on receiving side 150 for distributing the packets to the buffers on receiving side 130-i, a header processing unit
15 140 for determining a DSCP indicative of priority in a network and an output line number as an identifier of a line for outputting the packet, a packet transmission circuit on receiving side 120 for reading out the packets from the buffers on receiving side 130-i, packet forwarding
20 processing means 110 for switching the packets based on the output line number, M buffers on transmission side 131-i (where $i = 1$ to M), a buffer selector on transmission side 151 for distributing the packets to the buffers on transmission side 131-i, a packet transmission circuit on

09535389 060200

transmission side 121 for reading out the packets from the buffers on transmission side 131-i, a packet transmission circuit 161 for performing processing to transmit the packets, and an output line 102 from which packets are
5 outputted.

Although Fig. 1 shows a pair of the input line 101 and the output line 102, the router 100 actually has a plurality of input lines 101 and output lines 102.

Fig. 3 shows one example of a format of each packet
10 employed in a network. The packet transferred in the network comprises a header unit 310 and a data unit 320. The header unit 310 comprises a source IP address (hereinafter called SIP) 311 indicative of a source address (address of a transmission terminal), a destination IP address
15 (hereinafter called DIP) 312 indicative of a destination address (address of a receiving terminal), a source port (hereinafter called SPORT) 313 indicative of a protocol or application program, a destination port (hereinafter called DPORT) 314, and a DSCP 315 indicative of priority within
20 the network. Further, the data unit 320 comprises user data 321 indicative of data for a user. While the header unit 310 also includes information such as protocol information of the other layer higher than IP protocol in except for the above information, processing to be described later can

0955339-060200

be applied to them in a manner similar to the above information.

Fig. 3 shows a format in a case where a protocol of a transport layer is a TCP (Transmission Control Protocol) or a UDP (User Datagram Protocol), and a protocol of a network layer is an IP (Internet Protocol). However, the other protocols, for example, IPX as a protocol of the network layer or the like may be also applicable.

Fig. 4 shows one example of a format of packets in the router 100 according to the present invention. The format of the packet in the router 100 has an internal header unit 330 added to the format of the packets transferred in the network. The internal header unit 330 comprises a packet length 331 indicative of a byte length of the packet, an input line number 332 as an identifier of a line to which the packet is inputted, and an output line number 333 as an identifier of a line for outputting the packet therethrough.

When a packet is inputted from the input line 101, the packet receiving circuit 160 adds the internal header unit 330 to the packet, counts a byte length of the packet, and writes the byte length and an identifier of the input line 101 to which the packet is inputted, into the packet length 331 and the input line number 332, respectively. Then, the

002090"060200
09585389

packet receiving circuit 160 stores the packet and at the same time transmits packet header information 11 comprised of the internal header unit 330 and the header unit 310 to the header processing unit 140. In this case, the output
5 line number 333 includes a meaningless value.

The bandwidth monitoring unit 141 in the header processing unit 140 determines a DSCP from the packet header information 11 and transmits packet DSCP information 12 comprised of the DSCP to the packet receiving circuit 160.
10 The routing processing unit 142 in the header processing unit 140 determines an output line 102, to which the received packet should be output, based on the DIP 312 included in the packet header information 11 and transmits it to the packet receiving circuit 160 as packet output line
15 information 13.

Upon receiving the packet DSCP information 12 and the packet output line information 13, the packet receiving circuit 160 writes these information into the DSCP 315 and the output line number 333 and transmits the received packets
20 to the buffer selector on receiving side 150. The buffer selector on receiving side 150 determines one of buffers on receiving side 130-i according to the value of the DSCP 315 and transmits the packet to the buffer on receiving side.

Each buffer on receiving side 130-i has a discard

09553369 060200

threshold 132-i and performs buffer storage control based on the value of the DSCP 315. According to the buffer storage control, when the DSCP of a received packet indicates a priority packet, the received packet is stored in the buffer on receiving side 130-i if the buffer on receiving side 130-i has an empty area, and the received packet is discarded if there is no empty area. When the DSCP indicates a non priority packet, the received packet is stored in the buffer on receiving side 130-i when the amount of packets already stored therein is equal to or less than the discard threshold 132-i, and the received packet is discarded even if the buffer on receiving side 130-I has an empty area when the amount of the packets already stored therein has exceeded the discard threshold 132-i.

The packet transmission circuit on receiving side 120 performs control for reading out the packets stored in the buffers on receiving side 130-i. As the read-out control, there are known priority queuing, weighted fair queuing, etc. According to the priority queuing, the packets are read out one after another in storing order thereof from the buffer on receiving side 130-i having a high priority as far as packets are stored in the buffer. When no packets are stored in the buffer on receiving side 130-I having a high priority, packets are read out in storing order thereof

002090-060200 09553309

5 In the present invention, QoS of priority packets in the router 100 is achieved by utilizing the buffer storage control and read-out control described above in combination.

Detailed operation of the bandwidth monitoring unit
141 according to the present invention will next be described

by referring to Fig. 2 and Figs. 5 through 7.

A network configuration supposed by the present invention will first be explained using Fig. 2.

Fig. 2 shows a network wherein enterprise networks
5 A:210, B:220, C:230 and D:240 are connected to one another
by an Internet 200. The Internet 200 comprises edge routers
A:202 and B:203 located at edges of the network, and a
backbone router 201 located at a core thereof. Gateway
routers A:211, B:221, C:231 and D: 241 are placed in gateways
10 to the Internet 200 within the enterprise networks A:210,
B:220, C:230 and D:240.

The router 100 of the present invention shown in Fig.
1 is used as the edge router A202 for checking or monitoring
a bandwidth of priority packets contracted between the
15 Internet 200 and the enterprise network A: 210. The gateway
router A: 211 of the enterprise network A: 210 has a boundary
marking case in which packets are transmitted without making
a distinction between priority and non priority destinations,
and a customer marking case in which packets are transmitted
20 distinguishing between priority and non priority
destinations.

The boundary marking case will first be explained.
Incidentally, the bandwidth monitoring unit 141
preferentially judges voice packets as priority packets in

00505389 060200

the present embodiment.

As an algorithm for monitoring a bandwidth, such a modified algorithm is used that a Leaky Bucket Algorithm for monitoring a bandwidth of fixed-length packets is expanded in order to monitor a bandwidth of variable length packets. The Leaky Bucket Algorithm has been described in, for example, Chapter 4.4.2 of The ATM Forum Specification version 4.0.

The Leaky Bucket Algorithm is a model of certain depth of leakage bucket with a hole. While the bucket is storing water therein, water leaks at a predetermined rate corresponding to a monitoring bandwidth, and a fixed amount or level of water corresponding to one cell is poured into the bucket upon arrival of each cell. The bucket has a depth for the purpose of allowing fluctuations of cell arrival. When the water is not overflowing the bucket, input cells are judged to comply with a contract bandwidth. If the water overflows the bucket, input cells are judged to violate the contract bandwidth. In the invention of the present application, the monitoring of the bandwidth for variable length packets is achieved by varying the amount of water to be poured into the bucket depending upon a arrival packet.

A block diagram of the bandwidth monitoring unit 141 is shown in Fig. 5. The bandwidth monitoring unit 141

comprises a bandwidth check table control unit 560, a bucket water level decision unit 510, a check result decision unit 520, a DSCP decision unit 530, a flow detection unit 540, and a bandwidth check table 550.

5 The flow detection unit 540 is a functional part
inherent in a router. In an ATM switch, a connection is
established in advance, and bandwidth monitoring control
information is read out according to a connection identifier
of each input cell. Further, the bandwidth monitoring unit
10 executes bandwidth monitoring through the use of the
bandwidth monitoring control information (connection
communication). On the other hand, since no connection is
established in advance in a router device, the router device
needs to have flow detecting means for determining a flow
15 identifier used as an alternative to the connection
identifier for each input packet according to information
or the like lying within a header with a view toward
performing the bandwidth monitoring by the router device
(connectionless communication). The router reads out
20 bandwidth monitoring control information corresponding to
the flow identifier and executes the bandwidth monitoring
by using the bandwidth monitoring control information.

Incidentally, in the specification of the present application, a packet identifying condition created by

5

Fig. 6 shows a format of the bandwidth check table 550.

10

20

i.e., a monitoring or check rate, a time stamp (TS) 604-j (sec) indicative of the previous arrival time of a packet which refers to the same bandwidth check control information entry 600-j, a count (CNT) 605-j (Byte) indicative of the amount or level of water stored in the bucket immediately after the bandwidth monitoring of the previous packet, a DSCP conformance (DSCPC) 606-j indicative of a DSCP of a packet judged as conformance by the bandwidth monitoring and transferred as a priority packet, and a DSCP non-conformance (DSCPN) 607-j indicative of a DSCP of a packet judged as non-conformance and transferred as a non priority packet. Incidentally, the THR-A 601-j and THR-B 602-j each indicative of the depth of the bucket satisfy the relations in $\text{THR-A } 601\text{-j} \geq \text{THR-B } 602\text{-j}$.

Fig. 7 shows a flowchart of the bandwidth monitoring unit 141.

Processing performed in the bandwidth monitoring unit 141 comprises bandwidth check start processing 700, bucket water level decision processing 710, check result decision processing 720, and DSCP decision processing 730. The later three kinds of processing are principally executed by the bucket water level decision unit 510, check result decision unit 520 and DSCP decision unit 530 respectively.

When the bandwidth monitoring unit 141 receives packet

002090-060200

header information 11, a packet length storage 522 of the check result decision unit 520 stores a packet length 331 therein, and the flow detection unit 540 stores a SIP 311, a DIP 312, a SPORT 313 and a DPORT 314 therein (Step 701).

5 In Step 702, the flow detection unit 540 performs flow detection based on the stored information and judges or determines a flow identifier corresponding to an identifier of a flow for each input packet, and a flow priority which indicates the priority of packets within the flow. Thus,
10 the flow detection unit 540 transmits flow identifier information 14 comprised of the flow identifier to the bandwidth check table control circuit 561 of the bandwidth check table control unit 560 and transmits flow priority information 17 comprised of the flow priority to a flow
15 priority storage 524 of the check result decision unit 520. In the present embodiment, the flow priority of voice packet is defined as priority and the flow priority of the other packets are defined as non priority so that voice packets are preferentially judged as the priority packets.

20 Upon receiving the flow identifier information 14, the bandwidth check table control circuit 561 creates an address for accessing the bandwidth check table 550 based on the flow identifier information 14 to thereby read out bandwidth check control information 600-j. Thereafter, THR-A: 601-j

09585389.060200

and THR-B: 602-j are transferred to a THR storage 523 of the check result decision unit 520, and POLR 603-j, TS 604-j and CNT 605-j are transferred to a POLR storage 513, a TS storage 514 and a CNT storage 515 of the bucket water level
5 decision unit 510. Then DSCPC 606-j and DSCPN 607-j are transferred to a DSCPC storage 532 and a DSCPN storage 533 of the DSCP decision unit 530, respectively (Step 703).

In the bucket water level decision processing 710, the bucket water level decision unit 510 determines the level
10 of water in a bucket (bucket water level) immediately preceding the input of each packet. A bucket water level decision circuit 511 first calculates the difference between the value of a timer 512 for counting the present time and TS 604-j (sec) in the TS storage 514 which indicates the
15 arrival time of the previous packet to obtain a time which has elapsed since the arrival of the previous packet (Step 711). Next, the bucket water level decision circuit 511 calculates the level of water (reduced water level of bucket) which has leaked from the arrival of the previous packet
20 (Step 712) by multiplying the elapsed time (sec) by the POLR 603-j (Byte/sec) in the POLR storage 513. Further, the bucket water level decision circuit 511 subtracts the reduced water level of the bucket from the CNT 605-j in the CNT storage 515 which indicates a bucket water level

0020990 6953389 060200

5

10

20

j, i.e., it is estimated that the water must overflow the bucket when additional water equivalent to the packet length is poured, the check result decision circuit 521 judges the input packet as a violation packet and transmits bandwidth
5 check result information 15 indicative of violation to the DSCP decision circuit 531 of the DSCP decision unit 530 and the bandwidth check table control circuit 561 of the bandwidth check table control unit 560 (Step 726). On the other hand, if the added value (bucket water level + packet
10 length) is equal to or smaller than the value of THR-A 601-j, the check result decision circuit 521 judges that the input packet as a conformance packet and transmits bandwidth check result information 15 indicative of conformance to the DSCP decision circuit 531 and the bandwidth check table control
15 circuit 561 and transmits the added value (bucket water level + packet length) to the bandwidth check table control circuit 561 as a bucket water level information 16 (Step 725).

When the result of reference in Step 722 is judged as non priority, the added value (bucket water level + packet
20 length) and the depth of a bucket THR-B 602-j for the non priority packets stored in the THR storage 523 are compared (Step 724). If the added value (bucket water level + packet length) is larger than the value of THR-B 602-j, Step 726 referred to above is executed. Otherwise (bucket water

09533369 060200

level + packet length \leq THR-B 602-j), Step 725 referred to above is executed.

Steps 722 and 724 are processed inherent in the present invention. When the enterprise network A210 is transmitting voice packets at a rate within the contract bandwidth, since no overflow occurs as far as the amount of water poured in the bucket corresponds to the voice packets only, some amount of packets other than the voice packets may be transferred using the remain of the contract bandwidth by judging them as conformance. On the other hand, when a user is transmitting voice packets at a rate greater than the contract bandwidth, the bucket always stores water over the threshold level THR-B 602-j. Therefore, in this case, only the voice packets are judged as conformance.

Upon receiving bandwidth check result information 15 indicative of conformance, the bandwidth check table control circuit 561 writes bucket water level information 16 and a count or value of the timer 512 into their corresponding CNT 605-j and TS 604-j as a bucket water level and an arrival time of the packet at the instant of the bandwidth monitoring (Step 727). The bandwidth check table control circuit 561 does not execute Step 727 referred to above when bandwidth check result information 15 indicative of violation is received.

0955339-060200

In the DSCP decision processing 730, the DSCP decision unit 530 determines a DSCP, based on the bandwidth check result information 15. When the bandwidth check result information 15 is judged as conformance, the DSCP decision circuit 531 judges the DSCP stored in the DSCPC storage 532 as a DSCP of the input packet and transmits packet DSCP information 12 comprised of the DSCP to the packet receiving circuit 160 (Step 731). When the bandwidth check result information 15 is judged as violation, the DSCP decision circuit 531 judges the DSCP stored in the DSCPN storage 533 as a DSCP of the input packet and transmits packet DSCP information 12 comprised of the DSCP to the packet receiving circuit 160 (Step 732).

The bandwidth monitoring device having the bandwidth monitoring function, according to the prior art 1, determines voice packets within a monitoring bandwidth (contract bandwidth) as priority packets while judging surplus voice packets over the monitoring bandwidth and packets other than the voice packets as non priority packets. When the traffics shown in Fig. 8(a) are inputted, the traffics observed after the prior art bandwidth monitoring are represented as shown in Fig. 8(b). Packets other than voice packets indicated by diagonally-shaded portions shown in Fig. 8(b) are transmitted as non priority packets

00229901 69555555

regardless of the fact that the real amount of priority packets stays within the monitoring bandwidth. Namely, a manager of the enterprise network A210 is not able to sufficiently utilize the contract bandwidth for the priority
5 packets.

Since the bandwidth monitoring unit 141 according to the present invention is newly provided with a threshold THR-B 602-j, it is able to judge some amount of packets other than voice packets as priority packets when the bandwidth
10 of the received voice packets is below the contract bandwidth and the bucket water level is less than the THR-B 602-j. Traffics observed after passing through the bandwidth monitoring by the bandwidth monitoring unit 141 of the present invention are shown in Fig. 8(c), which indicates
15 that the manager of the enterprise network A210 can sufficiently utilize the contract bandwidth.

The above-described embodiment has described a case in which the gateway router A211 transmits two types of packets (voice packets and the other packets) different in
20 flow priority. A description will next be made of a case in which four types of packets different in flow priority are transmitted.

In the following embodiment, the gateway router A: 211 transmits four types of packets different in flow priority,

09585389.060200

such as packets of voice, transaction data, E-mail, and others. Incidentally, for example, priorities are given in order of voice > transaction data > E-mail > others.

Fig. 9 is a block diagram of a bandwidth monitoring unit 941, Fig. 10 shows a format of a bandwidth check table 950, and Fig. 11 is a flowchart of check result decision processing 1120, respectively. A description will be made of the difference between the transmission of the four types of packets and the transmission of the two types of packets.

As compared with the bandwidth check table 550, the bandwidth check table 950 is newly provided with THR-C 1008-j (where $j = 1$ to N) and THR-D 1009-j. Incidentally, there is a relation of $\text{THR-A } 601-j \geq \text{THR-B } 602-j \geq \text{THR-C } 1008-j \geq \text{THR-D } 1009-j$.

When the flow priority of packets are classified into four types, a flow detection unit 940 applies Step 1102 for determining a flow identifier and flow priorities (priority 1 to priority 4), transmitting flow identifier information 14 comprised of the flow identifier to a bandwidth check table control circuit 561 of a bandwidth check table control unit 560, and transmitting flow priority information 20 including one of said four flow priorities to a flow priority storage 924 in place of Step 702. Further, Step 703 is replaced by Step 1103 for storing even THR-C 1008-j, THR-D

09535389 060200

1009-j in a THR storage 923 in addition to the THR-A 601-j and THR-B 602-j.

Steps 722 through 724 of the check result decision processing 720 are respectively replaced by Steps 1122 through 1126 of check result decision processing 1120 shown in Fig. 11. In Step 1122, the flow priority storage 940 stores therein the flow priority information 20 transmitted by the flow detection unit 940, and processing operation is divided into four branches depending upon the stored information. When the stored information are respectively given as priority 1, priority 2, priority 3, and priority 4, THR-A 601-j, THR-B 602-j, THR-C 1008-j, and THR-D 1009-j are respectively compared in magnitude with added value of the bucket water level and packet length calculated in Step 721, and a decision as to either conformance or violation is made (Steps 1123 through 1126).

When the gateway router A: 211 transmits the four types of packets different in flow priority as described above, these packets can be packed into the contract bandwidth in order from the packets high in flow priority as shown in Fig. 12 owing to the bearing of four bucket's depths by the edge router A: 202. Similarly, when the gateway router A: 211 transmits H (> 2) types of packets different in flow priority, these packets can be packed into the contract

09585389 060200

A description has been made so far of the operations of the bandwidth monitoring unit 141 and the bandwidth monitoring unit 941 in the boundary marking case in which the enterprise network A: 210 transmits the packets without drawing the distinction between the priorities. A description will next be made of the operation of the bandwidth monitoring unit 141 in the customer marking case in which the enterprise network A: 210 transmits the packets while distinguishing between the priorities thereof.

In the boundary marking case, when the bandwidth monitoring unit 141 receives the packet header information

11 in Step 701, the flow detection unit 540 has stored the
SIP 311, DIP 312, SPORT 313 and DPORT 314 therein. In the
customer marking case, on the other hand, the DSCP 315
included in the header unit 310 is also stored in addition
5 to the above information and used for flow detection.
Operation other than these is identical to the operation
of the bandwidth check unit 141 in the boundary marking case.

Since the DSCP of each non priority packet is not
changed in the prior art 2 even when the gateway router A:
10 211 does not transmit the priority packets, the manager of
the enterprise network A: 210 could not effectively utilize
the contract bandwidth (see Fig. 13(b)). On the other hand,
when the router 100 provided with the bandwidth monitoring
unit 141 according to the present invention is used as the
15 edge router A: 202, the manager of the enterprise network
A: 210 can effectively utilize the contract bandwidth owing
to a rise in priority of the DSCP of the non priority packets
when the gateway router A: 211 transmits priority packets
at a rate less than the contract bandwidth (see Fig. 13(c)).

20 The embodiments illustrated up to now have described
the bandwidth monitoring of the connectionless
communication. A block diagram of a bandwidth monitoring
unit 1441 employed in a connection communication, such as
an ATM and a frame relay, is shown in Fig. 14.

09585389 060200

In the bandwidth monitoring unit 1441, the flow detection unit 540 shown in Fig. 9 is replaced by a connection priority decision unit 1440. The connection priority decision unit 1440 determines a connection priority which
5 indicate the priority of packets within a connection, based on a connection identifier within connection identifier information 18 and packet header information 11 and transmits the connection priority to a connection priority storage 1424 as connection priority information 19.

10 A bandwidth check table control circuit 1461 generates the address of one of entries in a bandwidth check table 550 based on the connection identifier used in place of the flow identifier to read out a bandwidth monitoring control information entry 600-j. Further, a check result decision
15 circuit 1421 judges the conformance or violation of the packet, based on the connection priority stored in the connection priority storage 1424. The other processing other than the above processing are identical to the operation of the bandwidth monitoring unit 141 employed in the
20 connection communication.

Although the priority of the network has been described while being limited to the DSCP of the IP header, a CLP (Cell Loss Priority) bit lying within a header of ATM cell and a DE (Delete Enable) bit lying within a frame header of a

002090" 6853550

5

10

20

5 packets are monitored by a node at the entrance of the network,
the following advantages are available.

0 the priority field of the other packets transmitted from
the user is automatically rewrite to a value corresponding
to the priority indication by a node located at the entrance
of the network, whereby the network operator can provide
a service which permits the effective use of the contract
5 bandwidth. By applying the bandwidth monitoring unit
having a function of rewriting the contents of the priority
field of non priority packets to a node at the entrance of
the network, such a bandwidth monitoring device is realized
that can offer a communication service in which the utility
0 efficiency of the contract bandwidth is improved.

According to the present invention, when the network user transmits packets to the network without setting the priority field, and the node at the entrance of the network determines priority packets and non priority packets

according to a priority packet decision policy contracted between the network operator and the network user, the following effects are brought about.

When it is found in the above decision that the
5 bandwidth of the priority packets is less than the limit
of contract bandwidth, by automatically changing the
contents of the priority field of packets judged as the non
priority packet to a value corresponding to that of the
priority packet, it is possible to provide a service which
10 permits the network user to effectively use the contract
bandwidth.

09585389 060200